TeleSeal Vendor Management Policy

Version: 1.0
Effective Date: 2025-07-27
Review Cycle: Annual
Owner: Chief Information Security Officer (CISO)

---

1. Purpose

To ensure that all third-party vendors supporting TeleSeal meet our security, privacy, and compliance requirements—including Arizona RON regulations (A.R.S. Title 2, Ch. 12, Art. 13).

2. Scope

Applies to all vendors, service providers, consultants, and contractors that:
- Process or store TeleSeal data (e.g., identity proofs, A/V streams, retention storage)
- Provide critical infrastructure or platform services (e.g., Authenticate.com, Twilio, AWS)
- Have logical or physical access to TeleSeal systems

3. Roles & Responsibilities

Role	Responsibility
CISO	Policy owner; approves vendor risk classification and exceptions
Vendor Management Team	Conduct vendor assessments; negotiate security requirements; manage ongoing reviews
Security Team	Evaluate vendor security posture; review SOC 2 reports and vulnerability scans
IT Operations	Integrate vendor services securely; enforce vendor access controls
Business Owner	Identify vendor business requirements; approve vendor selection

4. Policy Statements

4.1 Vendor Inventory & Classification

1. **Inventory:** Maintain a centralized register of all vendors, including:
   - Vendor name, service description, point of contact
   - Data domains accessed (e.g., identity data, recordings, certificates)
2. **Risk Classification:** Tier vendors into Low, Medium, or High risk based on:
   - Data sensitivity they handle (Public, Internal, Confidential, Restricted)
   - Criticality of service to TeleSeal operations
   - Regulatory or compliance impact

4.2 Due Diligence & Onboarding

- **High-Risk Vendors:**
  - Obtain and review latest SOC 2 Type II report, penetration test summary, and information-security questionnaire.

  - Conduct a security questionnaire covering data handling, encryption, incident response, and business continuity.

- **Medium-Risk Vendors:**
  - Review SOC 2 Type I report or equivalent security certification.
  - Confirm basic security posture (encryption in transit/at rest, MFA for access).

- **Low-Risk Vendors:**
  - Verify organizational details and non-disclosure agreement (NDA).

4.3 Ongoing Monitoring & Review

- **Annual Reviews:**
  - High-risk vendors: review updated SOC 2 reports and penetration test results
  - Medium-risk vendors: confirm continued certification or self-attestation

- **Quarterly Check-ins:**
  - Validate vendor performance against SLAs
  - Review security alerts or incidents involving the vendor

- **Access Reviews:**
  - Verify that vendor-issued accounts and credentials are current; revoke any unnecessary access

5. Offboarding & Termination

- **Access Revocation:** Immediately revoke all vendor access (credentials, API keys, network) upon termination.
- **Data Return/Destruction:** Ensure vendor returns or securely destroys all TeleSeal data.
- **Post-Engagement Review:** Document lessons learned and update Vendor Risk Register.

6. Exceptions

- Exceptions to this policy must be:
  1. Documented with rationale and compensating controls
  2. Reviewed and approved by the CISO
  3. Time-bound with scheduled re-evaluation

7. Enforcement & Sanctions

- Non-compliance may result in service suspension or termination.
- Repeat failures can trigger removal of vendor from approved list and tighter oversight for future engagements.

8. Review & Updates

- Reviewed annually, or upon:
  - Major regulatory changes (e.g., Arizona RON updates)

- Findings from audits or security incidents
- Introduction of new critical vendors or services

End of TeleSeal Vendor Management Policy